VOICE SCRAMBLING FOR RADIO, CELLULAR & TELEPHONE SYSTEMS

A. Bateman, J. D. Marvill & J. P. McGeehan
Centre for Communications Research, University of Bristol
Queens Building, University Walk
Bristol BS8 1TR, U.K.
Tel: +44 272 303104, Fax: +44 272 255265

Abstract – **A half-duplex analogue speech scrambler for radio communications pioneered by the University of Bristol and developed under licence to GEC-Marconi Secure Radio Systems has recently been designated by the Home Office as the sole scrambler recommended for use within the UK police. It employs a novel frequency-based scrambling technique, capable of maintaining a very high level of privacy and voice quality with negligible time delay. Designed for use in the mobile environment, rugged performance is achieved with the application of forward error correction during synchronisataion and key variable transfer. The scrambler is implemented on a low-cost, general purpose, single-chip digital signal processor (DSP). Minimal reduction in radio battery life is achieved through power management techniques. The same scrambling technique has been applied to fixed and cellular telephones, in full-duplex operation.**

1 Introduction

The majority of existing communications links - whether fixed or wireless - do not employ security measures to deter eavesdropping. Radio transmissions are particularly vulnerable since cheap scanning radio receivers are readily available, and are commonly used to compromise cellular telephone and private mobile radio (PMR) conversations. In the UK, one of the largest users of radio communications, the police, are moving to rectify the situation, by adopting a speech scrambler, to make their broadcasts unintelligible to unauthorised listeners. Extensive trials have recently been undertaken by the Home Office, with only one unit meeting the requirements necessary for recommendation. This paper describes some of the techniques developed and issues addressed in the design of the speech scrambler, which is based on a prototype developed at the University of Bristol.

2 Choice of Scrambling Techniques

The most important properties of a speech scrambler are:

- effectiveness in preventing readthrough
- quality of recovered (unscrambled) speech
- time delay introduced by processing
- bandwidth expansion
- level of security offered by encryption technique,
- ruggedness of synchronisation
- ease of production
- cost

The time delay issue, above any other parameter, determines the type of voice processing that can be applied in the scrambler. Conventional re-ordering

0-7803-0673-2/92 $3.00 1992 IEEE

of speech segments in the time domain can provide a very high degree of privacy, but incurs a significant time delay penalty. This arises from the need for all speech segments in a frame to be recovered before the original voice passage can be replayed, Fig 1. In general, the longer the interleaving period for the time domain based scrambler, the higher the level of privacy afforded. Delays of several hundred milliseconds are typically required. For application to half duplex radio systems, where radios are keyed on and off frequently, and messages are short, the time delay experienced by these devices can lead to operational difficulties for the users.

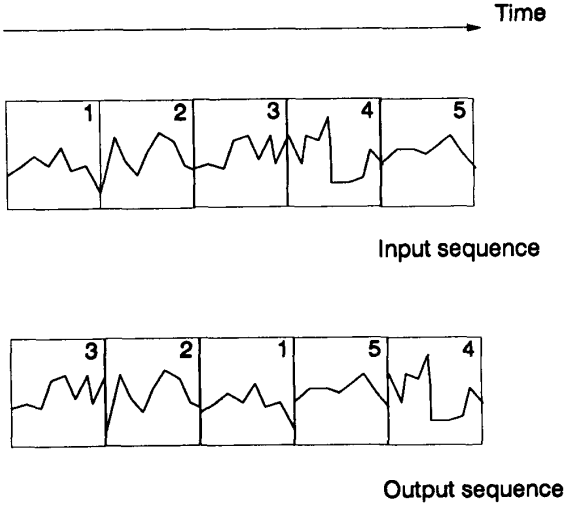

Figure 1: *Time domain scrambling*

To achieve a low time delay scrambler, signal manipulation in the frequency domain is the most widely used approach, with techniques ranging from simple frequency inversion, to multi-band reordering schemes, Fig 2. To achieve comparable levels of privacy to those offered by time domain techniques, the multi-band approach must be adopted, with the bands re-arranged in a rapid and suitably randomised manner. The success of a frequency domain scrambler is thus largely dictated by the number of bands used, the algorithm for their re-ordering, the speed of re-ordering, the precision with which the bands can be replaced, and the cost and complexity of implementation. In all of these areas it is believed that the new scrambling technique can claim a number of advances.

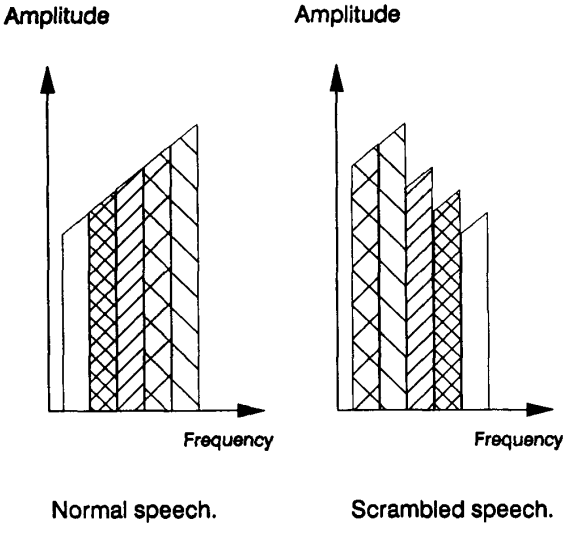

Figure 2: *Frequency domain scrambling*

3 Prototype Scrambler System

Much of the improvement in the new scrambler is achieved by the use of Digital Signal Processing (DSP) for realisation of the scrambling process. Not only does this allow precise, fast and repeatable frequency manipulation to be performed, but is also permits the incorporation of sophisticated synchronisation techniques to ensure very accurate and reliable reconstruction of the voice signal.

4 Crypto Engine

The basic processing performed by the DSP is illustrated in Fig 3. One of the key blocks is the "crypto engine", generating the stream of variables which control the pseudo-random reordering of the voice frequency. The integrity of the crypto engine is critical in achieving a high level of privacy for the scrambler. A number of connected shift register sequence generators are used in the device, arranged

such that it is impossible to deduce the seed key variable from a knowledge of the output variable sequence.

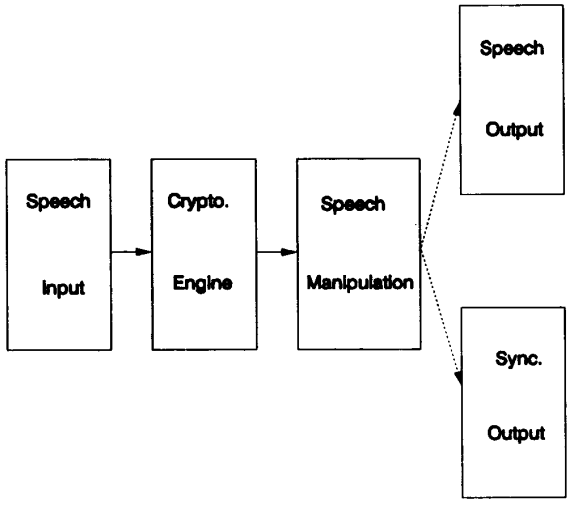

Figure 3: *DSP processing in transmit*

5 Speech Manipulation

Manipulation of speech based on the control variables forms the next major processing block. There are two well documented methods for spectral reordering: The Fast Fourier Transform can be applied to obtain frequency domain samples which can then simply be re-indexed. Alternatively, a filter bank can be used, similar to that employed for sub-band coding, with subsequent band re-positioning by conventional phasing techniques. The latter approach is used in the new scrambler, offering a much reduced implementation overhead and processing delay than the FFT approach.

6 Synchronisation

The final processing block is dedicated to achieving time synchronisation between the scrambling and de-scrambling functions. With the rapid reordering of the speech bands, a very precise synchronisation process is needed. From subjective analysis of the scrambler system, it is found that a synchronisation error of less than 5 ms must be maintained in order to preserve voice quality.

The initial method of synchronisation investigated involved detecting the phase reversal of a tone centred in the speech band. This approach had the attraction of a very simple implementation, and was based on the knowledge that notching out a small portion of the speech energy would have a negligible effect of speech quality. The presence of the tone also served the purpose of identifying that the unit was operating in secure mode. When tested in the scrambler system, the technique was found to work well under good signal strength conditions, but was prone to large synchronisation timing errors when the received signal strength fell and noise energy corrupted the tone. A more significant problem was observed when the radio units were tested with repeater systems, where intermodulation between the synchonisation tone and speech components not only corrupted the timing reference, but also resulted in an audible distortion of the recovered speech signal.

To eliminate these problems, a burst synchronisation scheme was adopted, based on a 1600 bps DPSK modem implemented in software. When a synchronisation update is needed, a short data burst is sent containing a known pattern which when correlated with the receiver reference pattern gives a precise timing reference. The timing error with this scheme was found to be less than one data bit period, ($\pm 1.25\ ms$).

In order to ensure unique reception of the synchronisation word in the presence of noise, a long word length is required, however this presents a conflict with the processing overhead involved in pattern matching, and the duration of the speech blanking imposed whilst synchronisation if performed. It is also possible that when operating in poor signal conditions with high bit error rates, the synchronisataion word will never be successfully decoded and synchronisation will be lost. A compromise solution was reached in the final design, by using

a synchronisataion word length of 31 bits with the addition of BCH forward error correction.

Under circumstances where synchronisation bursts were undetected due to severe signal fading, a "flywheeling" process was employed which maintained synchronisation based on an internal timer within the DSP. The accuracy of this flywheeling was sufficient to preserve voice quality for several tens of seconds before clock drift became too severe.

The frequency of synchronisataion bursts for a scrambler intended for mobile radio use is determined primarily by the requirement for "late entry" operation, where users either miss an initial synchronisation word due to fading or simply being out of range, or where users switch on their equipment during a call. The main factor which determines the minimum resync period is the subjective effect of frequent signal blanking during the data bursts. Based on customer trials, the maximum acceptable resync period was found to be three to four seconds. With the present scrambler design, this period can be altered under software control to suit specific customer needs.

To further enhance the security of the scrambler, a temporary key variable, termed the "initialisation vector", is transmitted with each resynchronisation burst. This is also protected by forward error correction, and changes the re-ordering process on a frame by frame basis. Thus, even if the scrambler sequence is deduced for a particular frame, the information is invalid for all subsequent frames.

7 Practical Implementation

As mentioned at the outset, the versatility and performance of the scrambler is greatly enhanced by the use of digital signal processing. In the prototype system, there are only two main peripheral devices, the codec for analogue I/O, and EEPROM for retention of key variables and customisation information.

With power consumption a key factor in a scrambler for use with portable radio equipment, the DSP chosen for the task was a first generation TMS320C17 processor from Texas Instruments. Through the use of novel algorithms, it was possible to implement the entire scrambler, modem, crypto engine and error correction processing on one device, with the entire unit consuming a current when active of only 35 mA. This value nevertheless is too high for many portable applications and a power down circuit was therefore added so that the device effectively switched off when the radio was in standby mode. Based on a typical 10% transmit, 10% receive and 80% standby duty cycle, the average current consumption is thus reduced to 7 mA from a 5V supply. With the device now available with a 3.5V specification, it is anticipated that power consumption can be reduced accordingly.

9 Performance

The University, in conjunction with GEC-Marconi Secure Radio Systems, has been a participant in a recent series of trials conducted by the UK Home Office to identify a scrambler for use by the UK police force. This trial was designed to asses a number of performance criterion including system reliability, privacy, quality, ease of use, and operational range. Of the five scrambler devices put forward for the trial, the scrambler based on the Bristol University algorithm was the sole device to receive Home Office approval.

8 Application of the scrambler to full duplex cellular and fixed telephone systems

In addition to the radio market, there is a growing requirement for scrambling on cellular and fixed telephone systems. For telephone operation, a full duplex mode of operation is required. To achieve this with a scrambler system, it is essential that all sidetone echo arising from 2:4 wire conversions at the handset and exchange is eliminated as this is

manifest as scrambled speech in the users earpiece. To eliminate sidetone in the telephone, a DSP based adaptive equaliser was developed, trained prior to the commencement of a call, which successfully eliminated all discernible echo. To preserve the subjective performance of the telephone system, an artificial, clear sidetone was generated within the DSP and passed to the users earpiece. In this application, a full duplex scrambler function was realised using a single TMS320C17 DSP, with the adaptive equaliser implemented in a second identical device.

9 Performance

The University, in conjunction with GEC-Marconi Secure Radio Systems, has been a participant in a recent series of trials conducted by the UK Home Office to identify a scrambler for use by the UK police force. This trial was designed to asses a number of performance criterion including system reliability, privacy, quality, ease of use, and operational range. Of the five scrambler devices put forward for the trial, the scrambler based on the Bristol University algorithm was the sole device to receive Home Office approval.

10 Conclusions

An overview of the requirements of a scrambler for use with mobile radio equipment has been presented. Details of the implementation of a scrambler are given satisfying these requirements, and which has recently won Home Office approval in the UK for use with the police forces. The scrambler is realised using general purpose DSP technology giving the benefits of low cost, high volume production with the flexibility of customisation and enhancement though software configuration.